

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,898	05/15/2001	Leonard Scott Veil	A33941 - 067668.0137	1161
21003	7590	07/16/2004	EXAMINER	
BAKER & BOTTS 30 ROCKEFELLER PLAZA NEW YORK, NY 10112			FOWLKES, ANDRE R	
			ART UNIT	PAPER NUMBER
			2122	

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	S
	09/855,898	VEIL ET AL.	
	Examiner Andre R. Fowlkes	Art Unit 2122	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 8/14/01.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-43 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-43 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ . |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>5/15/01</u> . | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

1. Claims 1-43 are pending.

Specification

2. The disclosure is objected to because of the following informalities: "verification process with fail" should be -- verification process will fail -- on p. 4 col. R line 1 of the PGPUB application.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-5, 7, 8, 14-21 and 33-36 are rejected under 35 U.S.C. 102(e) as being anticipated by Sprague et al. (Sprague), U.S. Patent no. 6,449,720.

5. The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

As per claim 1, Sprague discloses a **method for securely installing an applet on a computer system having a data storage and a secure processor** (col. 2:11, "security applets ... are loaded into ... the crypto unit (i.e. a computer system having data storage and a secure processor)'), **comprising:**

- **receiving an applet in a data storage** (col. 2:11, "security applets ... are loaded (i.e. stored) into ... the crypto unit (i.e. a computer system having data storage)'),

- **determining from at least a portion of the applet whether the applet is capable of being executed by a secure processor** (col. 2:27-31, "The crypto unit and the system of which it is a part, provides its secure internal environment (such that) only some security applets are (capable and) granted permission to load and run inside the crypto unit (i.e. secure processor)'),

- installing the applet on the secure processor if the secure processor is capable of executing the applet (col. 2:27-31, "The crypto unit and the system of which it is a part, provides its secure internal environment (such that) only some security applets are (capable and) granted permission to load and run inside the crypto unit (i.e. secure processor)").

As per claim 2, the rejection of claim 1 is incorporated and further, Sprague discloses that **the applet is stored in a non-secure storage** (fig. 1, item 30, "encrypted applet 1" stored in "hard drive (i.e. non-secure storage)", item 26, and associated text (e.g. col. 4:58 – col. 6:4)).

As per claim 3, the rejection of claim 2 is incorporated and further, Sprague discloses that **the applet further comprises a meta-data portion and an executable portion** (col. 3:16-17, "assigning a serial number (i.e. meta-data) and a cryptographic code key to the approved security applet (i.e. executable)").

As per claim 4, the rejection of claim 3 is incorporated and further, Sprague discloses that **the applet further comprises a certificate portion** (col. 7:30, "digital certificates (are) used to authenticate").

As per claim 5, the rejection of claim 3 is incorporated and further, Sprague discloses that the meta-data portion further comprises:

- a security meta-data portion (col. 11:61, “(the cryptographic meta data of an applet includes a) signature”),
- a resource meta-data portion which designates any resources required by the applet for execution (col. 11:43-45, “(the cryptographic meta data of an applet includes) size (field, that indicates how much of the memory resource is needed for the applet)”),
- a meta-data signature portion (col. 11:61, “(the cryptographic meta data of an applet includes a) signature”).

As per claim 7, the rejection of claim 5 is incorporated and further, Sprague discloses that **the step of determining whether the applet is capable of being executed by the secure processor further comprises loading the meta-data portion of the applet into a secure storage area in the secure processor** (col. 15:20-24, “(the system) inspects (the meta-data to determine if the applet is capable of being executed by the secure processor)... while simultaneously ... loading (the applet) ”).

As per claim 8, the rejection of claim 7 is incorporated and further, Sprague discloses that **the step of determining whether the applet is capable of being executed by the secure processor further comprises cryptographically verifying the security meta-data portion and the resource meta-data portion of the meta-data portion of the applet against the signature portion of the meta-data portion of**

the applet (col. 14:37-39, “The crypto unit uses the contents of the signature registry to determine whether each of the previously stored cryptographic contexts (i.e. the security and resource meta data of the applet) will be allowed to load and run.”).

As per claim 14, the rejection of claim 3 is incorporated and further, Sprague discloses: **an encrypted executable** (col. 3:21, “the encrypted security applet”); **and an unencrypted signature** (col. 9:28-29, “a manipulation detection code is a digital signature appended to (the applet”)).

As per claim 15, the rejection of claim 14 is incorporated and further, Sprague discloses that **the step of installing the applet on the secure processor further comprises storing the executable portion of the applet in the secure storage area** (col. 2:27-31, “The crypto unit ... provides its secure internal environment (i.e. storage), only some security applets are granted permission to load and run”).

As per claim 16, the rejection of claim 15 is incorporated and further, Sprague discloses that the step of installing the applet on the secure processor further comprises **requesting a decryption key for the encrypted executable portion of the applet; receiving the decryption key; and decrypting the encrypted executable portion into an unencrypted executable portion using the decryption key** (col. 3:57-60, “the crypto unit will (request and) receive from the OPC the cryptographic keys needed to decrypt and run the ... applet”).

As per claim 17, the rejection of claim 16 is incorporated and further, Sprague discloses that **the step of installing the applet on the secure processor further comprises verifying the unencrypted executable portion against the unencrypted executable signature** (col. 10:12-16, “the computed MAC … is compared with the received MAC. If the computed MAC and the Received MAC are equal, then … the decrypted security applet (is allowed to execute)”).

As per claim 18, the rejection of claim 16 is incorporated and further, Sprague discloses that **the step of installing the applet on the secure processor further comprises verifying the executable portion prepended with an applet serial number, against the unencrypted executable signature** (col. 14:37-39, “The crypto unit uses the contents of the signature registry to determine whether each of the previously stored cryptographic contexts (i.e. executable portion of the applet and serial number) will be allowed to load and run.”, and fig. 9A, and associated text (e.g. col. 14:30-15:7), shows unencrypted executable portion (i.e. the output from item 922) verified with the MAC (i.e. signature), via outputs from 928 and 934).

As per claim 19, the rejection of claim 17 is incorporated and further, Sprague discloses that the step of installing the applet on the secure processor further comprises **binding the unencrypted executable portion to the secure processor** (col. 14:4-6, “Since each client key is unique to each crypto unit, the swapped out cryptographic

context stored in the hard drive may not be swapped back into another crypto unit. (it is bound to its specific secure processor (i.e. crypto unit))").

As per claim 20, the rejection of claim 17 is incorporated and further, Sprague discloses that the step of installing the applet on the secure processor further comprises:

- encrypting the unencrypted executable portion to an encrypted executable (col. 5:28-29, "encrypting the ... security applet"),
- storing the encrypted executable in the non-secure storage (col. 5:40-41, "The hard drive (i.e. non-secure storage) typically holds a plurality of encrypted security applets"),
- storing the encrypted executable's decryption key in the secure storage area (fig. 1, and associated text (e.g. col. 4:55-6:4), item 21, "cryptographic operations center (i.e. secure storage)", stores the encrypted executable's decryption key).

As per claim 21, the rejection of claim 1 is incorporated and further, Sprague discloses that **the computer system further comprises a non-secure processor** (col. 5:44-45, "desktop PC further includes standard PC components such as a modem (and) CPU (i.e. a non-secure processor").

As per claims 33-36, Sprague also discloses such claimed limitations as addressed in claims 3-5 above, respectively.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 6, 9-13, 22-32 and 37-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sprague, U.S Patent No. 6,449,720 in view of Chefalas et al. (Chefalas), U.S. Patent Application Pub No. 2004/0015961.

As per claim 6, the rejection of claim 5 is incorporated and further, Sprague doesn't explicitly disclose that the resource meta-data portion is adapted to designate resources **comprising at least one of: a biometric sensor; a secure output; a keyboard; a personal identification number entry device; a global positioning system input; a magnetic stripe card reader; a secure storage area; a performance metrics, an algorithm implementing specific cryptographic algorithms; and at least one smart card slot.**

However, Chefalas, in an analogous environment, discloses that the resource meta-data portion is adapted to designate resources **comprising at least one of: a biometric sensor; a secure output** (p. 3 col. L:30-31, "Secure Sockets Layer (SSL)

technology"); a keyboard; a personal identification number entry device; a global positioning system input; a magnetic stripe card reader; a secure storage area; a performance metrics, an algorithm implementing specific cryptographic algorithms; and at least one smart card slot (p. 2 col. R:34-35, "(verifying that) the (system contains the appropriate) hardware (and software)... for the (selected) piece of software").

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time the invention was made, to incorporate the teachings of Chefalas into the system of Sprague in order to have a the resources designated, comprise at least one of : **a biometric sensor; a secure output; a keyboard; a personal identification number entry device; a global positioning system input; a magnetic stripe card reader; a secure storage area; a performance metrics, an algorithm implementing specific cryptographic algorithms; and at least one smart card slot.** The modification would have been obvious because one of ordinary skill in the art would have wanted verify that the appropriate requirements are available on the computer system in order to load the appropriate applet for the computer system, so that the applet/system combination will execute properly, (Chefalas, p. 1 col. R:32-39).

As per claim 9, the rejection of claim 7 is incorporated and further, Sprague doesn't explicitly disclose that **the step of determining whether the applet is capable of being executed by the secure processor further comprises verifying that a secure processor security requirement of the security meta-data portion of the**

applet is met or exceeded by a secure processor security rating of the secure processor.

However, Chefalas, in an analogous environment, discloses that **the step of determining whether the applet is capable of being executed by the secure processor further comprises verifying that a secure processor security requirement of the security meta-data portion of the applet is met or exceeded by a secure processor security rating of the secure processor** (p. 2 col. R:34-35, "(verifying that) the hardware (processor security requirements exceed the) ... prerequisites for the piece of software (i.e. the applet)").

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time the invention was made, to incorporate the teachings of Chefalas into the system of Sprague to have **the step of determining whether the applet is capable of being executed by the secure processor further comprise verifying that a secure processor security requirement of the security meta-data portion of the applet is met or exceeded by a secure processor security rating of the secure processor**. The modification would have been obvious because one of ordinary skill in the art would have wanted to load the appropriate applet for the specified computer system, based on all of the requirements of the applet program, so that the applet/system combination will execute properly, (Chefalas, p. 1 col. R:32-39).

As per claim 10, the rejection of claim 9 is incorporated and further, Sprague doesn't explicitly disclose that the step of determining whether the applet is capable of being executed by the secure processor further comprises:

- determining that the secure processor security requirement of the security meta-data portion of the applet is not met or exceeded by a secure processor security rating of the secure processor,**
- suggesting the use of a second applet that may have a second secure processor security requirement that is met or exceeded by the secure processor security rating of the secure processor.**

However, Chefalas, in an analogous environment, discloses that the step of determining whether the applet is capable of being executed by the secure processor further comprises:

- determining that the secure processor security requirement of the security meta-data portion of the applet is not met or exceeded by a secure processor security rating of the secure processor** (p. 2 col. R:4-9, "The verification process (uses the security metadata of the software to) determine whether target computers are capable (and composed of the required resources to) execute the desired software"),
- suggesting the use of a second applet that may have a second secure processor security requirement that is met or exceeded by the secure processor security rating of the secure processor** (fig. 11, item 1130, "does such (an applet)

version (that meets the requirements), exist?", and 1150, "(if such a version exists,) download proper version", and associated text (e.g. p. 3 col. R:51 -p. 4 col. L:7).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time the invention was made, to incorporate the teachings of Chefalas into the system of Sprague to have the step of determining whether the applet is capable of being executed by the secure processor further comprises:

- determining that the secure processor security requirement of the security meta-data portion of the applet is not met or exceeded by a secure processor security rating of the secure,**
- suggesting the use of a second applet that may have a second secure processor security requirement that is met or exceeded by the secure processor security rating of the secure processor.**

The modification would have been obvious because one of ordinary skill in the art would have wanted to load the appropriate applet for the specified computer system, based on all of the requirements of the applet program, so that the applet/system combination will execute properly, (Chefalas, p. 1 col. R:32-39).

As per claim 11, the Sprague/Chefalas system also discloses such claimed limitations as addressed in claim 9, above.

As per claim 12, the rejection of claim 7 is incorporated and further, Sprague doesn't explicitly disclose that **the step of determining whether the applet is capable**

of being executed by the secure processor further comprises verifying that the secure processor is capable of supplying resources designated in the resource meta-data portion of the meta-data portion of the applet.

However, Chefalas, in an analogous environment, discloses that **the step of determining whether the applet is capable of being executed by the secure processor further comprises verifying that the secure processor is capable of supplying resources designated in the resource meta-data portion of the meta-data portion of the applet** (p. 2 col. R:4-9, "The verification process (uses the resource metadata of the software to) determine whether target computers are capable (of supplying the resources designated to) execute the desired software").

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time the invention was made, to incorporate the teachings of Chefalas into the system of Sprague to have **the step of determining whether the applet is capable of being executed by the secure processor further comprises verifying that the secure processor is capable of supplying resources designated in the resource meta-data portion of the meta-data portion of the applet**

The modification would have been obvious because one of ordinary skill in the art would have wanted to load the appropriate applet for the specified computer system, based on all of the requirements of the applet program, so that the applet/system combination will execute properly, (Chefalas, p. 1 col. R:32-39).

As per claim 13, the Sprague/Chefalas system also discloses such claimed limitations as addressed in claim 10, above.

As per claim 22, Sprague discloses:

- receiving an applet in a non-secure data storage (col. 2:11, “security applets ... are loaded (i.e. stored) into ... the crypto unit (i.e. a computer system having non-secure data storage”),

-said applet comprises: a meta-data portion (fig. 4 items 316, 312, 310 and associated text, (e.g. col. 9:13-10:24),

said meta-data portion comprises:

- a security meta-data portion (col. 9:28-29, “a manipulation detection code is a digital signature appended to (the applet”),

- a meta-data signature portion (col. 9:28-29, “a manipulation detection code is a digital signature appended to (the applet”),

- an executable portion (col. 9:14, “applet”),

- installing the applet on the secure processor if the secure processor is capable of executing the applet (col. 2:27-31, “The crypto unit and the system of which it is a part, provides its secure internal environment (such that) only some security applets are (capable and) granted permission to load and run inside the crypto unit (i.e. secure processor”).

Sprague doesn't explicitly disclose that:

- said meta-data portion comprises a resource meta-data portion which designates any resources required by the applet for execution,

- determining whether the applet is capable of being executed by a secure processor based at least in part on the security meta-data portion and the resource meta-data portion of the applet, comprises:

- verifying that a secure processor security requirement of the security meta-data portion of the applet is met or exceeded by a secure processor security rating of the secure processor,

- verifying that the secure processor is capable of supplying the resources designated in the resource meta-data portion of the meta-data portion of the applet.

However, Chefalas, in an analogous environment, discloses that:

- said meta-data portion comprises a resource meta-data portion which designates any resources required by the applet for execution (p. 2 col. R:4-9, "The verification process (uses the resource metadata of the software to) determine whether target computers are capable (and composed of the required resources to) execute the desired software"),

- determining whether the applet is capable of being executed by a processor based at least in part on the security meta-data portion and the resource meta-data portion of the applet (p. 2 col. R:4-9, "The verification process (uses the resource and security metadata of the software to) determine whether target

computers are capable (and composed of the required resources to) execute the desired software"),**comprises:**

- verifying that a secure processor security requirement of the security meta-data portion of the applet is met or exceeded by a secure processor security rating of the secure processor (p. 2 col. R:34-35, "(verifying that) the hardware (processor security requirements exceed the ... prerequisites for the piece of software (i.e. the applet)'),

- verifying that the secure processor is capable of supplying the resources designated in the resource meta-data portion of the meta-data portion of the applet (p. 2 col. R:4-9, "The verification process (uses the resource metadata of the software to) determine whether target computers are capable (of supplying the resources designated to) execute the desired software").

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time the invention was made, to incorporate the teachings of Chefalas into the system of Sprague to have:

-said meta-data portion comprises a resource meta-data portion which designates any resources required by the applet for execution
- determining whether the applet is capable of being executed by a processor based at least in part on the security meta-data portion and the resource meta-data portion of the applet comprises:

- verifying that a secure processor security requirement of the security meta-data portion of the applet is met or exceeded by a secure processor security rating of the secure processor

- verifying that the secure processor is capable of supplying the resources designated in the resource meta-data portion of the meta-data portion of the applet

The modification would have been obvious because one of ordinary skill in the art would have wanted to load the appropriate applet for the specified computer system, based on all of the requirements of the applet program, so that the applet/system combination will execute properly, (Chefalas, p. 1 col. R:32-39).

As per claims 23-32, the Sprague/Chefalas system also discloses such claimed limitations as addressed in claims 1, 8, 10-16, 20 and 24, above.

As per claims 37-40, the Sprague/Chefalas system also discloses such claimed limitations as addressed in claim 22, above.

As per claim 41, the rejection of claim 38 is incorporated and further, Sprague discloses that **the resource meta-data portion comprises an applet serial number** (fig. 4 item 310, applet "serial number", and associated text, (e.g. col. 9:55-10:25).

As per claims 42 and 43, the Sprague/Chefalas system also discloses such claimed limitations as addressed in claim 8, above.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andre R. Fowlkes whose telephone number is (703)305-8889. The examiner can normally be reached on Monday - Friday, 8:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Q. Dam can be reached on (703)305-4552. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ARF



ANTONY NGUYEN-BA
PRIMARY EXAMINER